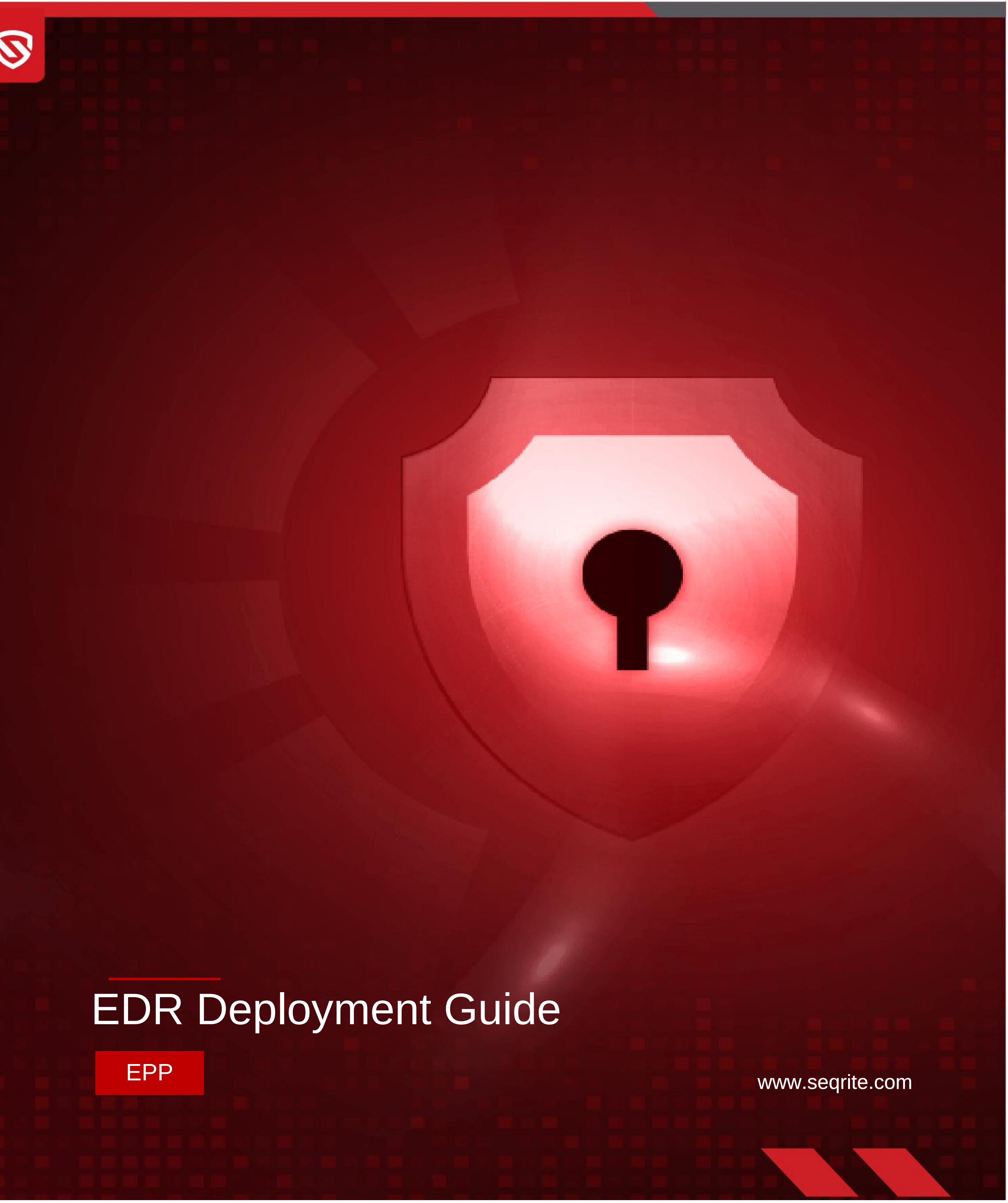
Seqrite

Endpoint Protection **EDR**



EDR Deployment Guide

EPP

www.seqrite.com

Copyright Information

Trademarks

License Terms

Contents

Overview 2

Audience 2

Prerequisites 2

System Requirements 2

Installation Steps 3

Troubleshooting 5

Overview

The Endpoint Detection and Response (EDR) is a platform deployed on an organization's own infrastructure rather than on cloud-based environment. It is a system designed to protect the endpoints from the network from potential cyber threats. EDR helps detect and responds to the threats that may evade the traditional antivirus and other security solutions deployed at the endpoint.

Audience

This guide is helpful for Seqrite Administrators and SOC Managers using EPP 8.3 with EDR edition.

Prerequisites

- EPP Server installed (Refer this link for the details on Installing EPP Server).
- EPP server with EDR license activated.
- EPP server must have Update Manager installed ensure internet connectivity in an air-gapped network.

System Requirements

EDR Server Supported OS

EDR Server only supports the Linux OS with Ubuntu 22.04 LTS server edition.

EDR Endpoint Supported OS

- Windows
    - Windows Server 2012, Core 2016 and 2019
    - Windows Server 2022, 2019, 2016
    - Windows 7, 8 (EPP), 10, 11
- Linux
    - CentOS 7.0+,
    - Red Hat Enterprise Linux (RHEL) 8.1 and later,
    - Mint 18.1 SUSE Linux 11.4+,
    - Ubuntu 18.04+,
    - BOSS 6,7,8

- Mac
  - Latest versions from and after Mac 10.15

Installation Steps

Ensure the system has the EPP 8.3 version with Endpoint Detection and Response (EDR) edition.

EDR edition in EPP 8.3 is a 2-step installation process.

- Extract the OPE folder and grant required permissions.
- Configure nodes and run the OPE services installed.

To extract the OPE folder installation folder, follow these steps

1. Create qh folder in var folder

sudo mkdir /var/qh

2. Extract ope-data-fresh.zip in /var/qh folder

sudo unzip /path/to/your/ope-data-fresh.zip -d /var/qh

3. Run this command to give required permissions

sudo chmod -R 777 /var/qh

All permissions are granted to configure the nodes and install OPE services

To configure the nodes, follow these steps

4. Open node configuration and navigate to nodes.json file location:

/var/qh/ope-data-fresh/install_config/.

5. Provide the following information in the nodes.json file: < Please provide dummy info on the below mentioned fields>

   - EPS IP Address: Enter the IP address to connect the EPS (Event Processing Server)
   - Hostname: Provide the VM hostname which is unique every time>>
   - Live Query URL: Enter a valid URL for live queries. << enter the dummy ip address>>
   - EPS Product Id: Enter the valid EPS product key
   - Domain: default domain is "*.ope.com"

   (Optional) To utilize the Organisation Certification Setup, mention the certificate name, key name, and domain name in the nodes.json file.

Restore the organization's certificate and key file to the directory at:

/var/qh/ope-data-fresh/certs

Note: Ensure that each node has a separate hostname that is included in the nodes.json file.

```
{
        "eps_ip": "178.15.18.43",
        "live_query_url": "",
        "cert_name": "“, << sample values- Piyush>>
        "cert_key_name": "",
        "domain": "*.ope.com",
        "eps_product_id": "Q9024D72345A8FA494",

            "enc_key":"DUMMYBgkqhkiG9DUMMYQEFAAOCAQ8AMIIBCgKCAQEAuSVztGN7KgtLcQggm8gsMfO8ATX2YaE+v6MWsuC3yb7xjLOcMM/MJ+UbEFhn2pClb",
            "api_key":"uSVzt13dummyN7KgtLcQgCE0cl5BzMvDuMmyMfO8ATX2YaE",
        "nodes": [
         {
           "ip": "171.18.3.21",
           "hostname": "OPEHOST21T",
           "user": "qhuser",
           "password": "pass123",
           "cpu": 4,
           "memory": 8,
           "memory_units": "GB",
           "disk": 1,
           "disk_units": "TB"
         }, {
           "ip": "171.18.3.22",
           "hostname": "OPEHOST22T",
           "user": "qhuser",
           "password": "pass123",
           "cpu": 16,
           "memory": 64,
           "memory_units": "GB",
           "disk": 1,
           "disk_units": "TB"
         }
       ]
     }
```

Ensure to run the below mentioned command manually.

1. Set the following environment variables.

   ```
   export TF_PLUGIN_CACHE_DIR="/var/qh/ope-data-fresh/components/tf_cache_dev/"
   ```

   ```
   export TF_CLI_CONFIG_FILE="/var/qh/ope-data-fresh/components/tf_cache/.terraformrc"
   ```

2. Run the following command to start installation.

   ```
   cd /var/qh/ope-data-fresh
   ```

   ```
   python3 fresh_install/main.py
   ```

Once the script is initiated, all OPE services begin running with the EPP environment configuration. The installation setup takes approximately 30-40 minutes.

EDR edition is now deployed in the EPP 8.3 version, along with the EPS registration and database access. The EPS database can be accessed through OPE services and vice versa.

Troubleshooting

To troubleshoot the deployment process, share all the generated log files with the Seqrite administrator. The log files created during the OPE installation script execution are restored in the local file location.